idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

CISPA Helmholtz Center for Information Security
Annabelle Theobald

01/03/2025
http://idw-online.de/en/news845262

Research results
Information technology
transregional, national

Digitaler Fingerabdruck: CSS eröffnet neue Möglichkeiten zum Nutzer:innen-Tracking

Prozessortyp, IP-Adresse, genutzter Browser, installierte Schriftarten – durch das Sammeln solcher und weiterer Merkmale der Browsereinstellungen und des zugrundeliegenden Betriebssystems lässt sich ein sehr genaues und in einigen Fällen sogar einzigartiges Profil von Nutzer:innen erstellen. Bekannt geworden ist dieses Phänomen als Browser Fingerprinting. Eine Untersuchung von CISPA-Forscher Leon Trampert und Kollegen legt jetzt nahe, dass dieses Trackingverfahren nicht nur beim Agieren im Web, sondern auch in Mails anwendbar ist und zwar auf einem bislang eher unterbeleuchteten Umweg: über den Einsatz von CSS (Cascading Style Sheets), einer Sprache zur Gestaltung von Websites.

Auch in einer großen Gruppe von Websitebesucher:innen sind Sie wahrscheinlich eindeutig identifizierbar. Warum? Überall dort, wo die Programmiersprache JavaScript zum Einsatz kommt – und das ist so ziemlich im gesamten Web – können auch spezifische Attribute zu den von Ihnen genutzten Geräten und deren Einstellungen gesammelt werden. Diese Infos sollen eigentlich Webentwickler:innen helfen, bessere Nutzererlebnisse und Funktionalitäten zu schaffen. Aber auch hier gilt: Wissen ist Macht und nicht jede:r will, dass dieses Wissen über ihn in der Welt ist. „Mittlerweile ist das Fingerprinting über JavaScript ziemlich bekannt. Menschen, denen Privatsphäre besonders wichtig ist, können sich schützen, indem sie JavaScript blockieren. Das geht entweder mithilfe von Plugins oder durch Nutzung des Tor-Browsers. Das kann zum Beispiel für Journalist:innen, die Angst vor Verfolgung haben, hilfreich sein“, erklärt Leon Trampert.

Modernes CSS lässt Daten durchsickern

Wo sich eine Tür schließt, geht eine andere auf, heißt es und so scheint es auch beim Fingerprinting zu sein. „Forschende haben kürzlich herausgefunden, dass auch durch den Einsatz von CSS Infos über Nutzende durchsickern können“, so Trampert. CSS (kurz für Cascading Style Sheets) sorgt dafür, dass Texte Bilder und Menüs an der richtigen Stelle stehen, es bestimmt Schriftarten und Farben sowie die Größe von Elementen auf Websites. Zudem hilft es, dass sich deren Ansicht an verschiedene Bildschirmgrößen anpassen können. „CSS wird immer beliebter und hat in den vergangenen Jahren immer neue Funktionen hinzugewonnen. Einige davon wurden von Forschungskolleg:innen bereits auf ihr Potenzial für Privatsphäre-Verletzungen untersucht. Eine ganzheitliche Betrachtung stand allerdings noch aus.“ Und so hatte sich Trampert vor einigen Monaten entschieden, systematisch moderne CSS-Funktionen zu untersuchen. „Wir wollten sehen, wie viel wir damit herausfinden können und ob CSS das Tracking auch jenseits des Webs ermöglicht.“

Verräterische Schriften

Trampert hat mehrere Fingerprinting-Ansätze untersucht und mithilfe verschiedener Techniken drei Wege aufgezeigt, mit denen mithilfe von CSS Fingerprints von Nutzenden erstellt werden können. „Wir haben zunächst 1176 Kombinationen aus Browser und Betriebssystemen mit verschiedenen Einstellungen untersucht und konnten in 97,95 Prozent Rückschlüsse auf das System der Nutzenden ziehen. Verräterisch sind zum Beispiel installierte Schriftarten. Sie

können Hinweise auf den genutzten Browser, das Betriebssystem und installierte Programme geben“, erklärt Trampert. Welche Schriftarten genutzt werden, haben die Forschenden mit ein paar Tricks herausgefunden: „Wir sehen das nicht im Klartext, können aber zum Beispiel durch das Ausnutzen bestimmter an sich sinnvoller CSS-Funktionen Höhen und Breiten von Wörtern messen und daraus nicht nur auf die Schriftart, sondern zum Beispiel auch auf die Systemsprache schließen“, sagt Trampert.

CSS erlaubt Tracking auch jenseits des Webs

Noch spannender war für ihn aber das Testen von Mailanwendungen. Denn während JavaScript von vielen Mailclients standardmäßig blockiert wird, ist der Einsatz von CSS bislang nicht begrenzt. „Wir haben 21 Mailclients untersucht, darunter sowohl Android- und iOS- als auch Desktop und Web-Clients. In neun Fällen konnten wir alle unsere Techniken erfolgreich einsetzen und so Informationen über die Nutzenden sammeln. 18 der 21 Mailclients davon waren für mindestens eine bestimmte Technik anfällig“, erklärt Trampert. Seiner Einschätzung nach könnte das ganz neue Bedrohungsszenarien eröffnen. „Angriffe könnten zum Beispiel darauf abzielen, die Web-Sitzungen von Besucher:innen mit deren E-Mail-Konto zu verknüpfen oder alle E-Mail-Adressen bestimmter Nutzer:innen zu identifizieren“, erklärt Trampert.

Und nun?

Wer sich im Web bewegt ist aufgrund des Einsatzes von Tracking-Cockies und JavaScript längst ungewollt vermessen. „Trotzdem ist es wichtig, aufzuzeigen, welche technischen Möglichkeiten es gibt und wo sich neue Missbrauchsmöglichkeiten eröffnen – wie hier gesehen plötzlich auch in Mailprogrammen. Nur so können wir auch robuste Verteidigungsmaßnahmen entwickeln“, sagt Trampert. Der PhD-Student forscht am CISPA betreut von den CISPA-Faculty Dr. Michael Schwarz und Prof. Dr. Christian Rossow und will sich auch in Zukunft weiter mit Mailsicherheitsfragen beschäftigen.

Original publication:

Trampert, Leon; Weber, Daniel; Gerlach, Lukas; Rossow, Christian; Schwarz, Michael (2025). Cascading Spy Sheets: Exploiting the Complexity of Modern CSS for Email and Browser Fingerprinting. CISPA. Conference contribution. https://doi.org/10.60882/cispa.27194472.v2

Visualisierung zum Paper "Cascading Spy Sheets: Exploiting the Complexity of Modern CSS for Email and Browser Fingerprinting"
CISPA